Indian Journal of Science and Technology, *Vol 7(3), 312–317, March 2014*
ISSN (Print) : 0974-6846
ISSN (Online) : 0974-5645

Possibility and Necessity Measures to Enhance Reliability and Cooperation in MANETS

Anoop J. Sahoo[1*] and Md. Amir Khusru Akhtar[2]

[1]Infosys Limited Chennai, India; anoop.jyoti88@gmail.com
[2]Department of Computer Engineering, Cambridge Institute of Technology, Ranchi, Jharkhand, India; akru2008@gmail.com

Abstract

Ensuring security in Mobile Ad hoc Network (MANET) is a major concern. The majority of attacks can be prevented by secure routing protocol, but non-cooperation still suffers from a serious drawback which is the total strength of nodes in a network. A lot of solution to enforce cooperation has been proposed in the literature which isolate nodes directly on the basis of lesser reputation values but reduces the total strength of nodes in a network. Finally, the lesser strength of nodes degrades the performance and reliability of mobile ad hoc networks.

To enforce cooperation in MANET this work presents the Perfect Evidence (PE) model which uses reputation value to obtain the possibility and necessity measures and isolate a node having perfect evidence. It involves nesting of focal element to know the perfect evidence. The proposed model enhances performance of the network because it eliminates only one misbehaving node in each turn, which maintains the total strength of nodes in a network. In addition to that it enhances cooperation in network because it identifies and isolates the most misbehaving node and warns other misbehaved nodes. The warning message suggests other misbehaving nodes to cooperate in network activities otherwise at any turn it will be isolated from the network. Experimental result shows the efficiency of the model.

Keywords: Evidence, Focal Element, Necessity Measure, Possibility Measure, Reputation Value

1. Introduction

A MANET is an independent body of mobile nodes connected by wireless links. These networks work in a standalone fashion in which each node has to cooperate in network activities. But, in order to save its valuable resources nodes drop packets of others which degrades the efficiency of packet transfer, increases the packet delivery time, enhances the packet loss rate and creates network partitioning. The packet dropping attack or misbehavior is further classified into selfish and malicious as discussed by Anusas-Amornkul[1]. In selfish misbehavior nodes drop packets of others for its honest causes such as battery life and bandwidth. In spite of that we have some malicious causes of data dropping attacks such as wormhole and blackhole. The other reason for data dropping attacks are network congestion, jamming and burst channel errors due to interference, fading etc. In this work, a node which drops packets of others is called a selfish node or misbehaving node.

This chapter presents the Perfect Evidence (PE) model which uses reputation value to obtain the possibility and necessity measures and isolate a node having perfect evidence. It involves nesting of focal element to know the perfect evidence. The proposed model involves one or more expert nodes which are accountable for all major computations, analysis and isolation of misbehaving nodes. We have used reputation values to analyse and isolate a node in each turn. In each turn we identify a single misbehaving node and warn other misbehaving nodes to cooperate in network activities. The identified misbehaving node is isolated from the routing paths. Our proposed model isolates only one node in each turns to maintain the total strength of nodes in a network which enhance

*Author for correspondence

network performance, because poor strength of nodes degrades the network performance. In addition to that it enhances cooperation in network because it identifies and isolates the most misbehaving node and warns other misbehaved nodes. The warning message suggests other misbehaving nodes to cooperate in network activities otherwise at any turn it will be isolated from the network. Experimental result shows the efficiency of the model.

The rest of this paper is organized as follows: Section 2 presents the related work and assumptions. Section 3 presents the PE model. Section 4 discusses the experiments and results. Finally, Section 5 concludes the paper.

2. Related Work and Assumptions

2.1 Related Work

The reputation-based mechanism is based on detection and punishment strategy. It maintains a reputation system in order to identify and punish selfish nodes. In a self organized network nodes are trustor as well as trustee. For a cooperative network reputation of a node is defined on the basis of network participation (i.e., routing and forwarding) of as seen by others. A lot of metrics are used to define the reputation of a node such as the packet delivery ratio and others. On the basis of reputation values nodes misbehave is identified and punished. The majority of attacks based on manipulation of routing data can be cured by secure routing protocol[2–7] but non cooperation or misbehavior is still in its natal stage.

To mitigate routing misbehavior several mechanisms are proposed in the literature such as Watchdog and Pathrater[8], CONFIDANT[9–10], CORE[11] and others[12–17]. The proposed Watchdog and Pathrater mechanism rewards selfish nodes because there is no punishment for misbehavior. The other mechanisms[9–17] prevent a network from misbehavior up to some extent. But, still faces a serious limitation which is the total strength of nodes in the network which degrades the network performance and reliability.

A lot of other mechanisms are proposed in the current literature to mitigate routing misbehave. A novel classification algorithm for the intrusion detection in MANET has been proposed by Mitrokotsa and Dimitrakakis[18]. But, this method is not validated with real world data. Hernandez–Orallo et al.[19–20] have proposed two efficient mechanisms for the detection of selfish nodes in MANET. But, these algorithms consume the valuable resources such as battery power and bandwidth which degrade the network performance. A secure routing protocol with selfishness resistance in MANETs has been proposed by Li et al.[21], but it also consumes the valuable resources which degrade the network performance.

2.2 Assumption

This work involves one or more expert nodes which are accountable for all major computations, analysis and isolation of misbehaving nodes. Expert nodes are the intelligent nodes of the ad hoc network having high computation capability and memory to process and store reputation values[22–23]. The reputation values are used to analyse and isolate a selfish node in a single turn. In each turn we identify a single misbehaving node and warn other misbehaving nodes to cooperate in network activities. The identified selfish node is eliminated from the routing paths. The list of cooperative nodes is broadcasted in the MANET which is used by existing solutions[9–12] in the routing activities. Our proposed model enhances performance of the network because it eliminates only one node in each turn thus maintain node strength. As we know that poor node strength degrades the network performance. In addition to that our model enhances cooperation in network because it identifies and eliminates the most misbehaving node and warns other misbehaved nodes. The warning message contains the identity of eliminated node and suggests other misbehaving nodes to cooperate in the network activities otherwise at any turn it will be isolated from the network. The proposed MANET is shown in Figure 1 in which an expert node is denoted by a laptop node which has high computation capability and battery life.

3. Perfect Evidence (PE) Model

This section presents the PE model. The proposed PE model uses reputation value to obtain the possibility and necessity measures[24–25] to know the perfect evidence of misbehavior. It involves nesting of focal element to know the perfect evidence. Where, focal element represents the element of the power set. We have involved one or more than one expert nodes responsible for all major computations, analysis and isolation of misbehaving nodes.

3.1 Introduction

To classify a network let us consider n number of nodes participating in a MANET. To know the perfect evidence,

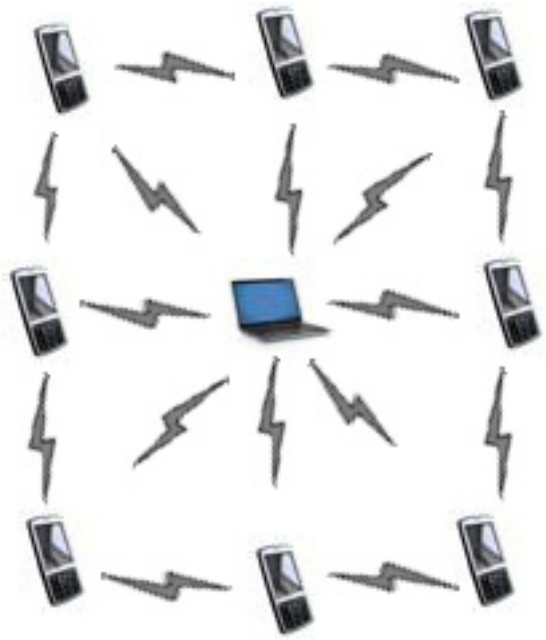

Figure 1. The proposed MANET with an expert node.

let us consider a collection of some or all of the nodes of the MANET in terms of the power set of a universe. If these sets are satisfying the property $N_1 \subset N_2 \subset N_3 \subset \cdots \subset N_n$, then according to Shafer[26] these sets are said to be nested. For the nested relationship the belief and plausibility measures are said to be a consonant body of evidence, because the evidence does not conflict. According to Klir and Folger[27] if two different sets A and B on the power set of a universe, i.e., if A, B $\in$ P(X) then the following relationships can be hold for a consonant body of evidence[24–25].

$$bel(A \cap B) = \min[bel(A), bel(B)] \quad (1)$$

$$pl(A \cup B) = \max[pl(A), pl(B)] \quad (2)$$

From Eqs. 1 & 2 it is clear that that the belief measure of the intersection of two sets is the minimum value of the belief measures of the two sets. On the other hand the plausibility measure of the union of these two sets is the maximum value of the plausibility measures of the two sets.

On the basis of the literature the consonant belief and plausibility measures are termed as necessity (ne) and possibility (po) measures[24–25]. Thus, Eqs. 1 and 2 can be written as

$$ne(A \cap B) = \min[ne(A), ne(B)] \quad (3)$$

$$po(A \cup B) = \max[po(A), po(B)] \quad (4)$$

Now, the dual relationships for a consonant body of evidence can be expressed as

$$po(A) = 1 - ne(\overline{A}) \quad (5)$$

$$ne(A) = 1 - po(\overline{A}) \quad (6)$$

At this instant, a possibility distribution is an ordered sequence of values.

$$r = (d_1, d_2, d_3, \ldots, d_n) \quad (7)$$

The belief measure can be calculated by expert node using

$$b_i = R_i / \sum_{i=1}^{n} R_i \quad (8)$$

The possibility measure can also be defined using the n-tuple which represent the basic distribution[24–25]

$$m = (b_1, b_2, b_3, \ldots, b_n) \quad 9)$$

$$\sum_{i=1}^{n} b_i = 1 \quad (10)$$

where $b_i \in [0, 1]$ and $b_i = m(N_i)$. Here, sets N_i are nested for the requirement to make consonant bodies of evidence which means misbehaving node n and its supportive nodes.

Now, d_i is calculated[24–25] as

$$d_i = \sum_{k=1}^{n} b_k = \sum_{k=1}^{n} mN_k \quad (11)$$

On that basis Eq. 11 can be expressed[24–25] as

$$\begin{aligned} d_1 &= b_1 + b_2 + b_3 + \cdots + b_n \\ d_2 &= \quad b_2 + b_3 + \cdots + b_n \\ d_3 &= \quad\quad b_3 + \cdots + b_n \\ &\quad\quad\quad \cdots \\ d_n &= \quad\quad\quad\quad b_n \end{aligned} \quad (12)$$

Thus, nesting of focal elements is an important attribute for the body of evidence. It is useful in MANET to know the perfect evidence of misbehavior, because it shows the relationship of a misbehaving node to other nodes.

3.2 Algorithm to Identify and Isolate Misbehaving Node

In this work reputation values are obtained from the literature[9–12]. Our proposed work involves possibility and necessity measures to eliminate a misbehaving node. This algorithm identifies and eliminates a misbehaving node in each turn. We can use as many turn as the network requires and on that basis assign value for Maximum Turn (MAXT). In this work expert nodes

are responsible for all major computations, analysis and isolation of misbehaving nodes. Thus, it gives a reduction in resource consumption because major computations are performed by expert nodes which save battery power of other nodes.

3.2.1 Algorithm: Perfect_Evidence

Step 1: Obtain reputation values of the i^{th} node (R_i) using any of the methods discussed[9–12].

Step 2: Repeat step 3 to 6 while R_i>=MAXT

Step 3: Calculate belief measure of the i^{th} node (b_i) and its nested sets using Eq. 8 as

$$b_i = R_i / \sum_{i=1}^{n} R_i$$

Step 4: Calculate the possibility distribution the i^{th} node (d_i) and its nested sets using Eqs. 11 & 12 as

$$d_i = \sum_{k=1}^{n} b_k$$

Step 5: Obtain smallest possibility distribution on the basis of Eqs. 9 & 10 and identify misbehaving node

Step 6: Eliminate misbehaving node and broadcast warning message

4. Experiments and Results

In order to obtain results we have performed an experiment to identify misbehaving nodes. Let us consider a MANET of eight nodes denoted by n_1–n_8. To determine the identity of the nodes the expert node aggregates these nodes into sets shown in Table 1. The third column shows the reputation value (R) of nodes where reputation values are taken from the literature[9–12]. In this work we have taken reputation values between 0 and 1 in place of the between 0 and 100[12]. For instance, if reputation value is 60 then it is taken 0.6. The fourth column shows the belief measure (b) calculated using Eq. 8 by expert node and the last column represent the possibility distribution (d) calculated from Eqs. 11 & 12.

A MANET of eight nodes with a border node is shown in Figure 2. It shows a group of regular nodes with one expert node. Regular nodes are the cooperative nodes of the network. The expert node is responsible for the major computations. The belief measure calculated by expert node for node n_1 and its nested sets is shown in Figure 2. We have shown a grid topology in Figure 1 which is the real topology for this work. The topology shown in Figure 2 is only to show the node n_1 and its nested sets.

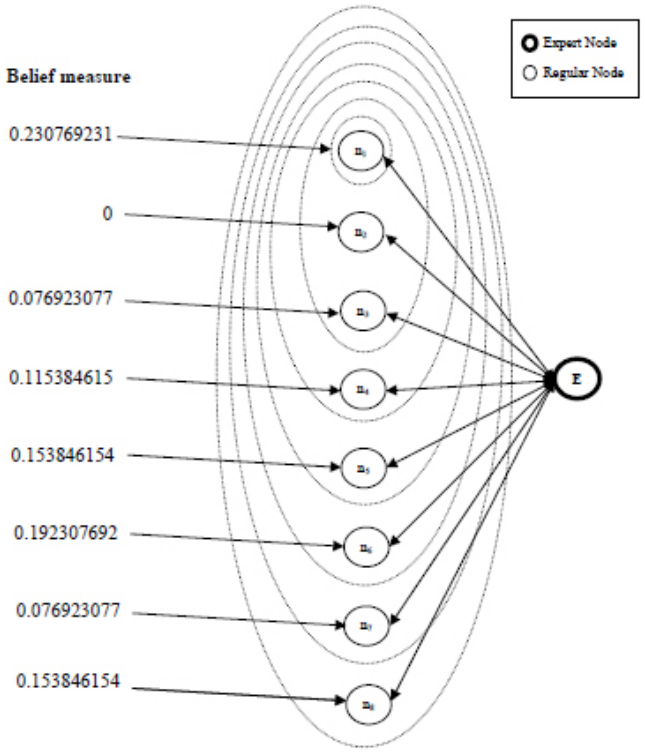

Figure 2. Nesting diagram for node n_1.

The importance of this nesting is that it uses belief measure to eliminate selfish node and warn other nodes to cooperate in routing activities. On the basis of Table 1, the belief measure is as high as 0.230769231 for set n_1 and as less as 0 for set $n_1 \cup n_2$.

After that the smallest possibility distribution of length 8 using Eq. 7 has the form r = (1, 0, 0, 0, ..., 0), where there are 7 zeros after a value of unity in the distribution. Similarly, the smallest basic distribution takes the form m = (1, 0, 0, 0, ..., 0). Now, we can analyse that there would be only one focal element having all the evidence. Thus, this complete evidence situation represents perfect evidence, because this case does not involve any uncertainty and shows that node n_1 is most misbehaving node. Finally, node n_1 is eliminated and a warning message is forwarded to other nodes.

A lot of reputation based mechanisms have been proposed in the literature which eliminates nodes from network participation having lesser reputation value resulting reduction in node strength. The reduction in node strength degrades the network performance. That's why this model does not directly eliminate nodes only on the basis of lesser reputation values. But, it uses probability and necessity measure to identify the most misbehaving

Table 1. Perfect evidence assignment

Set	Focal Element	R	b	D
N_1	n_1	0.6	0.230769231	1
N_2	$n_1 \cup n_2$	0	0	0.769230769
N_3	$n_1 \cup n_2 \cup n_3$	0.2	0.076923077	0.769230769
N_4	$n_1 \cup n_2 \cup n_3 \cup n_4$	0.3	0.115384615	0.692307692
N_5	$n_1 \cup n_2 \cup n_3 \cup n_4 \cup n_5$	0.4	0.153846154	0.576923077
N_6	$n_1 \cup n_2 \cup n_3 \cup n_4 \cup n_5 \cup n_6$	0.5	0.192307692	0.423076923
N_7	$n_1 \cup n_2 \cup n_3 \cup n_4 \cup n_5 \cup n_6 \cup n_7$	0.2	0.076923077	0.230769231
N_8	$n_1 \cup n_2 \cup n_3 \cup n_4 \cup n_5 \cup n_6 \cup n_7 \cup n_8$	0.4	0.153846154	0.153846154

The basic distribution is $\sum_{i=1}^{8} b_i = 1$

nodes and eliminate a single node in each turn and warn other nodes. The warning message suggests the selfish nodes to cooperate in the network activities otherwise at any turn it will be eliminated.

5. Conclusion

Due to the infrastructure less design, a MANET is most vulnerable to attacks and misbehavior. To enforce cooperation this paper suggests the possibility and necessity measure to know the perfect evidence. The proposed model involves one or more expert nodes which are accountable for all major computations, analysis and isolation of misbehaving nodes. We have used reputation values to analyse and isolate a node in each turn. In each turn we identify a single misbehaving node and warn other misbehaving nodes to cooperate in network activities. The identified misbehaving node is isolated from the routing paths. Our proposed model isolates only one node in each turn to maintain the total strength of nodes in a network which enhance network performance, because poor strength of nodes degrade the network performance. In addition to that it enhances cooperation in network because it identifies and isolates the most misbehaving node and warns other misbehaved nodes. The warning message suggests other misbehaving nodes to cooperate in network activities otherwise at any turn it will be isolated from the network. Experimental result (table 1) shows the efficiency of the model.

6. References

1. Anusas-Amornkul T. On detection mechanisms and their performance for packet dropping Attack in ad hoc networks [PhD Thesis]. ProQuest; 2008.
2. Hu YC, Johnson DB, Perrig A. SEAD: Secure efficient distance vector routing for mobile wireless ad hoc networks. Ad Hoc Networks. 2003; 1(1):175–92.
3. Hu YC, Perrig A, Johnson DB. Ariadne: A secure on-demand routing protocol for ad hoc networks. Wireless Networks. 2005; 11(1–2):21–38.
4. Papadimitratos P, Haas ZJ, Samar P. The Secure Routing Protocol (SRP) for ad hoc networks. Proceedings of the 2nd ACM Workshop on Wireless Security; 2002. p. 41–50.
5. Sanzgiri K, Dahill B, Levine BN, Shields C, Belding-Royer EM. A secure routing protocol for ad hoc networks. Proceedings of the 10th IEEE International Conference on Network Protocols; 2002. 78–87.
6. Sanzgiri K, LaFlamme D, Dahill B, Levine BN, Shields C, Belding-Royer EM. Authenticated routing for ad hoc networks. IEEE J Sel Area Comm. 2005; 23(3): 598–610.
7. Zapata MG, Asokan N. Securing ad hoc routing protocols. Proceedings of the 1st ACM Workshop on Wireless Security; 2002. p. 1–10.
8. Marti S, Giuli TJ, Lai K, Baker M. Mitigating routing misbehavior in mobile ad hoc networks. Proceedings of the 6th Annual International Conference on Mobile Computing and Networking (Mobicom); 2000. p. 255–65.
9. Buchegger S, Le Boudec JY. Nodes bearing grudges: towards routing security, fairness, and robustness in mobile ad hoc networks. Proceedings of the 10th Euromicro Workshop on Parallel, Distributed and Network-based Processing; 2002. p. 403–10.
10. Buchegger S, Le Boudec JY. Performance analysis of the CONFIDANT protocol. In Proceedings of the 3rd ACM international symposium on Mobile ad hoc networking & computing; 2002. p. 226–36.
11. Michiardi P, Molva R. CORE: a collaborative reputation mechanism to enforce node cooperation in mobile ad hoc networks. In Advanced Communications and Multimedia Security; 2002; US: Springer. p. 107–21.

12. Balasubramanian A, Ghosh J. a reputation based scheme for stimulating cooperation in MANETs. Proceedings of the 19th International Teletraffic Congress; Beijin g; 2005.
13. Bansal S, Baker M. Observation-based cooperation enforcement in ad hoc networks [Internet]. 2003. Available from: arXiv preprint cs/0307012
14. Buttyán L, Hubaux JP. Stimulating cooperation in self-organizing mobile ad hoc networks. Mobile Network Appl. 2003; 8(5):579–92.
15. Akbani R, Korkmaz T. Enhancing role-based trust management with a reputation system for MANETs. EURASIP Journal on Wireless Communications and Networking. 2011; 2011:1–14.
16. Wang F, Wang F, Huang B, Yang LT. COSR: a reputation-based secure route protocol in MANET. EURASIP Journal on Wireless Communications and Networking. 2010; 2010: 1–11.
17. Zakhary SR, Radenkovic M. Reputation-based security protocol for manets in highly mobile disconnection-prone environments. Proceedings of the 7th International Conference on Wireless On-demand Network Systems and Services (WONS); 2010 Feb. p. 161–67.
18. Mitrokotsa A, Dimitrakakis C. Intrusion detection in MANET using classification algorithms: The effects of cost and model selection. Ad Hoc Networks. 2013; 11(1):226–237.
19. Hernandez-Orallo E, Olmos M DS, Cano JC, Calafate CT, Manzoni P. Evaluation of collaborative selfish node detection in MANETS and DTNs. Proceedings of the 15th ACM international conference on Modeling, analysis and simulation of wireless and mobile systems. 2012. p. 159–66.
20. Hernandez-Orallo E, Serrat MD, Cano J, Calafate CT, Manzoni P. Improving selfish node detection in MANETs using a collaborative watchdog. IEEE Communications Letters. 2012; 16(5):642–45.
21. Li CT, Yang CC, Hwang MS. (2012). A secure routing protocol with node selfishness resistance in MANETs. International Journal of Mobile Communications. 2012; 10(1):103–18.
22. Saeed N. Intelligent MANET optimisation system [Ph.D Thesis]. Brunel University; 2011.
23. Saeed NH, Abbod MF, Al-Raweshidy HS. IMAN: an intelligent MANET routing system. Proceedings of the IEEE 17th International Conference on Telecommunications (ICT); 2010. p. 401–04.
24. Ross TJ. Fuzzy logic with engineering applications. 3rd ed. UK: John Wiley & Sons; 2009.
25. Klir G, Yuan B. Fuzzy sets and fuzzy logic: theory and applications. Upper Saddle River, NJ: Prentice Hall; 1995.
26. Shafer G. A mathematical theory of evidence. Princeton, New Jersey: Princeton University Press; 1976.
27. Klir G, Folger T. Fuzzy sets, uncertainty, and information. Englewood Cliffs, NJ: Prentice Hall; 1988.